UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,602	07/30/2001	Christopher P. Jalbert	04860P2441	5216

7590 07/14/2005

James C. Sheller
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/918,602	**Applicant(s)** JALBERT ET AL.	
	Examiner Kevin Schubert	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 May 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *05162005*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claims 1-41 have been considered.

Information Disclosure Statement

The information disclosure statement filed 5/16/05 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because an NPL entry has not been submitted. Examiner could not find cited reference "SPEKE: A Strong Password Method". The IDS has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609 ¶ C(1).

Claim Objections

Claims 2 and 8 are objected to because of the following informalities: "secrete" is misspelled. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-6 and 20-22 are rejected under 35 U.S.C. 102(b) as being anticipated by Vogelesang, U.S. Patent No. 5,953,424.

As per claims 1,20,21, and 22, the applicant describes a cryptographic method with the following limitations which are met by Vogelesang:

a) receiving at a first entity a second public key M_A (Col 16, lines 33-38);

b) generating a first session key K_B based on the second public key M_A (Col 16, lines 39-42);

c) generating a first random nonce N_B (Col 16, lines 64-67);

d) encrypting the first random nonce N_B using at least a first password P_B and a first public key M_B to obtain an encrypted random nonce (Col 16, lines 64-67);

e) transmitting the encrypted random nonce from the first entity (Col 16, lines 64-67);

f) receiving a response to the encrypted random nonce (Col 17, lines 19-24);

g) authenticating through determining whether the response includes a correct modification of the first random nonce (Col 17, lines 28-30);

As per claim 2, the applicant describes the method of claim 1, which is met by Vogelesang, with the following limitations which are also met by Vogelesang:

a) generating a first secrete S_B from at least the first password P_B and the first public key M_B (Col 16, lines 39-42);

b) encrypting the first random nonce N_B using at least the first secrete S_B (Col 16, lines 64-67);

The applicant should note that the session key and the first secret both are met by shared secret S in Vogelesang.

As per claims 3 and 4, the applicant describes the method of claim 2, which is met by Vogelesang, with the following limitation which is also met by Vogelesang:

Checking whether a received modification of the first random nonce equals a modification of the first random nonce as applied to the first random nonce by the first entity (Col 17, lines 25-37);

As per claim 5, the applicant describes the method of claim 2, which is met by Vogelesang, with the following limitation which is also met by Vogelesang:

a) generating a first random number R_B (Col 16, lines 39-40);

b) computing the first session key K_B from the second public key M_A raised to the exponential power of the first random number R_B, modulo a parameter B_B (Col 16, lines 39-42).

As per claim 6, the applicant describes the method of claim 2, which is met by Vogelesang, with the following limitation which is also met by Vogelesang:

Wherein the first secret S_B is generated using a combining function f_B on at least the first password P_B and the first public key M_B (Col 8, lines 7-10).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 24,26-27, and 38-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Schneier (Schneier, Bruce. Applied Cryptography. John Wiley & Sons. 1996. Washington DC. Pages 4-5 and 357).

As per claims 24 and 38-40, the applicant describes a cryptographic method comprising the following limitations which are met by Vogelesang and Schneier:

a) receiving at a first entity a second public key M_A and an encrypted second random number (Vogelesang: Col 16, lines 33-38; lines 64-68);

b) generating a first session key K_B based on the second public key M_A (Vogelesang: Col 16, lines 39-42);

c) decrypting using at least a first password P_B and the second public key M_A to retrieve a second random number N_A from the encrypted second random number (Vogelesang: Col 17, lines 1-18);

d) modifying the second random number N_A to obtain a modified second random number (Vogelesang: Col 17, lines 19-24);

e) encrypting the modified second random number using at least the first password P_B and a first public key M_B to obtain an encrypted random package (Vogelesang: Col 7, lines 19-24; Schneier: pages 4-5);

f) transmitting the encrypted random package from the first entity (Vogelesang: Col 17, lines 25-27).

Vogelesang discloses all the limitations of the above claim except for encrypting the modified second number at the first entity using a first password **and** a first public key (part e). Vogelesang discloses the use of passwords, such as K and J factors, which are used to construct the shared secret (session key) which is used to encrypt the modified second random number. However, Vogelesang discloses that the session key at the first entity is constructed using a received second public key and a password, not a first public key and a password.

Schneier discloses the idea of public key cryptography in which a message may be encrypted using a recipient's public key so that only the corresponding private key of the recipient may decrypt the message (Schneier: pages 4-5). Schneier also discloses the idea that a message may be doubly encrypted with two keys to enhance security (Schneier: pages 357). Combining the ideas of Schneier into the system allows the modified second number to be encrypted with a first session key as prescribed by Vogelesang and then doubly encrypted with a recipient's public key (ie a first public key) thereby satisfying the limitations of part e. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneier with those of Vogelesang to increase security through double encryption.

As per claim 26 and 27, the applicant describes the method of claim 24, which is met by Vogelesang in view of Schneier, with the following limitations which are met by Vogelesang:

a) generating a first random number R_B (Col 16, lines 39-40);

b) computing the first session key K_B from the second public key M_A raised to the exponential power of the first random number R_B, modulo a parameter B_B (Col 16, lines 39-42).

Claims 7-13,17-19,24,26-32,34-37 and 38-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Vanstone, U.S. Patent Application No. 2001/0042205.

As per claims 24 and 38-40, the applicant describes the following limitations which are met by Vogelesang in view of Vanstone:

a) receiving at a first entity a second public key M_A and an encrypted second random number (Vogelesang: Col 16, lines 33-38; lines 64-68);

b) generating a first session key K_B based on the second public key M_A (Vogelesang: Col 16, lines 39-42; Vanstone: [0046]-[0062]);

c) decrypting using at least a first password P_B and the second public key M_A to retrieve a second random number N_A from the encrypted second random number (Vogelesang: Col 17, lines 1-18);

d) modifying the second random number N_A to obtain a modified second random number (Vogelesang: Col 17, lines 19-24);

e) encrypting the modified second random number using at least the first password P_B and a first public key M_B to obtain an encrypted random package (Vogelesang: Col 7, lines 19-24; Vanstone [0046]-[0062]);

f) transmitting the encrypted random package from the first entity (Vogelesang: Col 17, lines 25-27).

Vogelesang discloses all the limitations of the claim except the session key generated in Vogelesang's system does not satisfy the limitations of part e. Vanstone discloses a similar cryptographic system in which a session key is generated based on first **and** second public keys (x and y) and a password such as a private key p_b.

Combining Vanstone with Vogelesang allows for the construction of a different session key which fuses both the first and second public keys and a password and not just one public key and a password as prescribed in the primary reference. It would have been obvious to one of ordinary skill in the art to combine the ideas of Vanstone with those of Vogelesang because doing so allows for the construction of a session key which is more secure since it combines the additional knowledge of an extra public key.

As per claims 26-28, the applicant describes the method of claim 24, which is met by Vogelesang in view of Vanstone, with the following limitation which is also met by Vanstone:

Using the combining function f_B on the first password P_B and on the second public key M_A and the first public key M_B (Vanstone: [0054] and [0055]).

As per claims 7-10 and 29-31, the applicant describes the method of claims 6,2, and 28, which are met by Vogelesang (6 and 2) and Vogelesang in view of Vanstone (28), with the following limitations which are also met by Vanstone:

a) combining the second public key M_A and the first public key M_B with the first password P_B to produce a first result (Vanstone: [0060]);

b) hashing the first result with a secure hash (Vanstone: [0060]);

The session key K, which is a function of first and second public keys (x and y), is combined with a^y which is a password to form a secure hash using a hashing algorithm (SHA-1). The examiner notes that the password is met in more than one way by Vanstone.

As per claims 11 and 32, the applicant describes the method of claims 2 and 27, which are met by Vogelesang in view of Vanstone, with the following limitations which are also met by Vanstone:

a) combining the first password P_B and at least one of the second public key M_A and the first public key M_B to generate a first combined result (Vanstone: [0060]);

b) combining the first combined result and at least one of the second public key M_A, the first password P_B, and the first public key M_B to generate a second combined result (Vanstone: [0060]);

The first combined result is the creation of the session key, and the second combined result is the hashing function.

As per claims 12 and 13, the applicant describes the method of claim 2, which is met by Vogelesang in view of Vanstone, with the following limitation which is also met by Vogelesang:

Wherein the first random nonce is encrypted using a symmetrical encryption algorithm (Col 16, lines 64-67).

As per claims 17-19 and 34-37, the applicant describes the method of claims 2 and 24, which are met by Vogelesang in view of Vanstone, with the following limitation which is also met by Vogelesang:

a) generating a first random number N_B (Vogelesang: Col 13, lines 41-57);

b) encrypting a combination of the first random number N_B and the modified second random number (Vogelesang: Col 13, lines 41-57).

The first random number is V, and the modified second random number is N.

As per claim 41, the applicant describes the method of claim 40, which is met by Vogelesang in view of Vanstone, with the following limitation which is also met by Vogelesang:

Wherein the network is a network operating according to a hypertext transfer protocol and the first public key M_B is transmitted for session key exchange before the encrypted second random number is received (Col 1, lines 12-14; Col 16, lines 25-67).

Claims 14-19,25, and 33-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Vanstone in further view of Schneier.

As per claims 14-19,25, and 33-37, the applicant describes the method of claims 2 and 24, which are met by Vogelesang in view of Vanstone, with the following limitation which is met by Schneier:

a) decrypting the encrypted second random number using the first session key K_B to generate a first decrypted result (Vogelesang: Col 17, lines 1-18);

b) decrypting the first decrypted result using at least the first password P_B and the second public key M_A (Vanstone: [0046] to [0062]; Schneier: page 357);

Vogelesang does not disclose the use of double encryption with two encryption keys. Vogelesang in view of Vanstone disclose the construction of two separate session keys. Schneier discloses the idea that two separate encryption keys can be used to doubly encrypt a message. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneier and Vanstone with those of Vogelesang because doing so allows for double encryption which enhances security.

Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang.

As per claim 23, the applicant describes the system of claim 22, which is met by Vogelesang, with the following limitation:

A network operating according to a hypertext transfer protocol and the first public key M_B is transmitted with the encrypted random nonce for session key exchange (Col 1, lines 12-14);

Vogelesang does not disclose transmitting the first public key M_B with the encrypted random nonce. The examiner takes official notice that it would have been obvious to one of ordinary skill in the art at the time the invention was filed to transmit a key with a nonce because doing so is more efficient than having to make two separation transmissions for the key and the nonce.

Response to Arguments

Applicant's arguments, see Remarks filed 5/16/05, with respect to claim 1 have been fully considered but they are not persuasive. The applicant argues that Vogelesang does not disclose part d. The examiner disagrees. Vogelesang discloses the use of encrypting a nonce with a session key which is constructed from a public key and a password (Col 16, lines 39-42). Vogelesang discloses a system in which a first participant generates a second public key, X (Col 16, lines 36-38). The first participant receives the second public key upon generation (part a), and then the first participant sends the second public key to the second participant.

The second participant generates a session key using the second public key (Col 16, lines 41-42) (part b). The first participant generates a first random nonce, L (Col 16, lines 64-67) (part c) and encrypts the first random nonce with the session key which is a function of a password and a first public key, Y (Col 16, lines 64-67) (part d). The first participant then sends the encrypted random nonce to the second participant who receives it and modifies it for authentication (Col 16, line 64 to Col 17, line 37).

Applicant's arguments with respect to claim 2 have been fully considered but they are not persuasive. The applicant argues that Vogelesang does not disclose generating a first secret. The examiner disagrees. Vogelesang discloses the generation of a shared secret S which is constructed from authentication factors K and J (passwords) and a first public key. The examiner notes that there is nothing to preclude the first session key from being the first secret as disclosed in the claim limitations.

Applicant's arguments with respect to claim 16 have been fully considered but they are not persuasive. The applicant argues that the transmission of private signal L does not include the transmission of public signal X. The examiner agrees. However, the examiner fails to see how this argument renders the claim patentable since this limitation is not in claim 16. Claim 16 relates to transmitting a first public key to a second entity to establish a session key which is clearly met by Vogelesang (Col 16, lines 33-35).

Applicant's arguments with respect to the rejection(s) of claim(s) 8,15,17,18,24,25, and 34 have been fully considered and are persuasive. Therefore, the rejection(s) have been withdrawn. However, upon further consideration, a new ground(s) of rejection is made.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137